the art cited by the Examiner has remained the same, the reasons given by the Examiner as to why the cited art renders, for example, claim 1 unpatentable has changed significantly. Applicants assert that the newly alleged combination of the cited art amounts to a new art grounds of rejection such that the Examiner is prohibited from making this Office Action final. (See MPEP 706.07(a)). Furthermore, the Examiner's reference to the teachings of Feistel has, in effect, included that reference in the art grounds of rejections such that the rejection should be construed as a new grounds of rejection. Accordingly, applicants respectfully request that the Examiner withdraw the finality of the December 27, 2000 Office Action.

In restating the art grounds of rejection, the Examiner makes several allegations, which construe the teachings of the cited references in an unduly broad manner. For instance, the Examiner contends that Schneier and Feistel teach that the use of look-up tables is standard practice in the cryptographic arts. Either the Examiner does not clearly understand the cited art or does not clearly understand the claims at issue. Claim 1 does not simply recite the use of a look-up table. Claim 1 recites "employing an enhanced tbox function using an involuntary lookup." The Examiner has not pointed to any disclosure or suggestion in either Schneier or Feistel that a lookup table should be used to employ an enhanced tbox function.

Furthermore, in a standard Feistel pass, repeats in a lookup table's input yield a linear relationship in the corresponding sum of the table's output and other intermediate cipher texts. This property allows certain types of cryptographic attacks. By contrast the invention as recited in claim 1 employs an "involuntary lookup" that does not have this linearity property and thus is immune from such attacks.

The Examiner also alleges that it is known to perform transformation on data streams before and after application of a cryptographic algorithm. However, this does not equate to permutations within the cryptographic algorithm itself. Namely, none of the art cited by the Examiner discloses or suggests "the inputs to the enhanced tbox function being subjected to a permutation using one or more of the secret offsets to produce a permutation result," as recited in claim 1.

Claim 1 is not rendered obvious to one skilled in the art by Alanara in view of Appendix A of IS-54, Schneier, Feistel, Vernan, Friedman and Reeds. If the Examiner maintains these rejections, applicants respectfully request that the Examiner specifically point out where in the art the use of an involuntary lookup for employing an enhanced tbox function can be found, and where in the art permuting the inputs to the enhanced tbox function using one or more secret offsets can be found.

Claims 2-18, alone or by their dependency on claim 1, includes similar limitations to claim 1, and are patentable at least for the reasons stated above with respect to claim 1.

In view of the above, applicants respectfully request that the Examiner withdraw the art grounds of rejection and allow the subject application.

In the event that any outstanding matters remain in this application, Applicant requests that the Examiner contact Gary D. Yacura (Reg. No. 35,416) at (703) 205-8071 to discuss such matters.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies to charge payment or credit any overpayment to Deposit Account No. 02-2448 for any additional fees required under 37 C.F.R. §§ 1.16 or 1.17; particularly, extension of time fees.

Very truly yours,

BIRCH, STEWART, KOLASCH & BIRCH, LLP

By _____
Gary D. Yacura
Reg. No. 35,416

GDY/kmr

P.O. Box 747
Falls Church, VA 22040-0747
(703) 205-8000